REMARKS

Applicants thank the Examiner for the thorough consideration given the present application. Claims 1-27 are currently being prosecuted. The Examiner is respectfully requested to reconsider his rejections in view of the remarks as set forth below.

Entry of Amendment

Applicants submit that since the present response includes only remarks, entry of the present response and full consideration by the Examiner are proper.

Rejections under 35 U.S.C. § 103

Claims 1-9, 12, 13, 18, 23, 26 and 27 stand rejected under 35 U.S.C. § 103 as being obvious over Rowney et al. (U.S. Patent 5,987,140) in view of Oishi (U.S. Patent 6,298,153). This rejection is respectfully traversed.

The Examiner states that Rowney shows a method for performing a transaction between legal entity A and legal entity B over network and that the transaction is initiated by legal entity A. The Examiner also states that Rowney discloses legal entity A associating a transaction with the verification insignia to verify the approval to legal entity B. Rowney further discloses that the verification insignia is a unique transistory insignia provided to A by C thereby guaranteeing that A has been approved. The Examiner admits that Rowney does not teach that the unique transistory insignia is valid for a single transaction and valid only for a sufficient time to complete a transaction. The Examiner also admits Rowney does not teach invalidating substantially immediately after the validation of the transistory unique insignia.

The Examiner recites the Oishi reference to teach a certificate that is valid only for a single transaction and valid only for a sufficient time to complete a transaction. The Examiner feels it would have been obvious to one of ordinary skill in the art to modify Rowney to use a certificate which is valid only for a single transaction and valid only for sufficient time to complete the transaction.

Applicants disagree with the Examiner's understanding of the references and submit that claim 1 is not obvious over this combination of references.

First, Applicants submit that the claimed invention as a whole must be considered in determining the differences between the prior art and the claims. Applicants submit that the claimed invention as a whole would not be obvious in the manner suggested by the Examiner.

Rowney discusses the objective of their invention in column 2, lines 44-56 as an approach which encourages the deployment of a three party secure channel such as SET. Rowney has invented a temporary hybrid solution based on the well-known SSL secure channel to provide incentive for customers to install SET compliance software. As stated by Rowney, customers do not want to deploy the SET hybrid standard as it is burdensome, complicated and requires a software program and a certificate being downloaded to the customer's computer. Even if Rowney's invention does not create a more secure environment for payment systems aimed at the Internet, it can not prevent purchases of services/goods using a stolen credit card number, which is still a very serious problem today.

In rejecting the claims, the Examiner refers to column 10, lines 4-19, column 10, lines 31-58 and column 11, lines 29-37. However, this section of the patent is a description of the SSL protocol and starting at column 10, line 33, it is direct copy of wording from the SSL protocol description paragraph 7.6.1.2 (Protocol Version 3.0, March 1996, can be found on the Internet at http://wp.netscape.com/eng/ssl3/ssl-toc.html). Based on the definition and description of the SSL protocol, it is clear that the SSL protocol does not deal with application data and does not process the contents of application data transactions, but merely transmits application data transactions transparently.

Thus, it could be stated that it is not possible to associate the described SSL certificate (X.509) with the payment transaction. The SSL certificate is part of protocol layer and there is no link between the protocol layer and the application layer.

Claim 1 deals with an application data transaction, such as a payment transaction between a legal entity A (for example, a customer computer) who has an approval to perform such a transaction to legal entity B (for example, a merchant computer) over a network, the transaction being initiated by A, wherein A associates the transaction with the verification insignia to verify the approval to B where the verification insignia is a unique transistory insignia such as a unique virtual credit card number. This insignia is provided to A by a legal entity C (for instance, a credit card company, a bank or other institution) who thereby guarantees that A has the approval. However, this insignia is conditioned by legal entity A providing to C a secret identification code such as a user identification and a password confirming the identity of A to C. B validates the transistory insignia, and upon positive validation and only then accepts the transaction. The transistory unique insignia is invalidated substantially immediately after the validation.

It is important to note that the certificate mentioned in the SSL protocol is an optional feature which means that the customer computer does not always have the certificate. Further, this is a X.509.v3 certificate which is issued by a certification authority and to obtain such a certificate, one must contact an authority and submit certain personal information in order to obtain the certificate. This normally takes on the order of hours or days.

The Examiner argues that the optional certificate described in the SSL protocol is the same as the unique transistory insignia of the present application. We believe this is incorrect because the unique transistory insignia is valid only for a single transaction and is only valid for a short time.

Furthermore, claim 1 is directed to a method for performing a transaction between A and B. Rowney does not disclose a method for performing a transaction between A that has an approval to perform such a transaction and B over a network. Rowney does not describe any transaction exchange between A and B or that A has an approval to perform such a transaction. Furthermore, Rowney depicts an overview of the invention and just mentions that the customer computer system is in communication with the merchant computer system using a general purpose secure communication protocol such as SSL. Rowney does not disclose anything about a transaction in the reference.

Claim 1 also states that the transaction is initiated by A. Rowney does not disclose that the transaction is initiated by A, but discloses that the communication is initiated by A. In the reference, the SSL protocol is described which does not contain or describe any exchanges of transactions. Transaction exchanges take place at the application level which is not part of the protocol and which is transparent for the SSL protocol.

Claim 1 describes that A associates the transaction with the verification insignia. Rowney does not disclose that A associates the transaction with the verification insignia to verify the approval to B, but discloses that the legal entity A optionally transmits a client certificate to

B. There is no mention of a data transaction. The certificate described must be obtained from a certificate authority which takes on the order of hours or days.

Claim 1 describes the insignia as being a unique transistory insignia which is valid for a single transaction and valid only for sufficient time to complete the transaction. Rowney does not disclose the verification insignia as a unique transistory insignia provided to A by C who thereby guarantees that A has approval, but instead discloses that B (the merchant computer) verifies C's (payment gateway computer system) public key certificate to verify the legal identity of C. Further, Rowney does not disclose that providing the unique transistory insignia to A by C is conditioned by A providing to C a secret identification code confirming the identity of A to C, but instead discloses that B creates the payment authorization request based on previously captured data such as the amount, the account number, and any additional data such as pass words needed to validate the charge. Rowney does not disclose that C provides A with a unique transistory insignia.

Claim 1 further states that B validates the unique transistory insignia and upon positive validation accepts the transactions. Rowney does not disclose that B validates the insignia and upon positive validation accepts the transaction but instead discloses that B verifies C's public key certificate to verify the legal identity of C.

Claim 1 further states that the transistory unique insignia is invalidated substantially immediately after the validation. Rowney does not disclose that the insignia is invalidated immediately after validation, but merely describes the SSL protocol. Furthermore, B is not able to invalidate a certificate issued to A by C.

The Oishi reference deals with digital signatures and public key systems and crypto systems and does not deal with any kind of secure payment system. The reference describes the use of an anonymous public key certificate (one-time certificate) mentioned in a very special situation but does not specify that it is only valid for a pre-specified time. The whole subject of the Oishi invention is very special cases of public key systems and digital signatures and has nothing to do with electronic payment systems. Thus, Applicants submit that it would not be obvious to use the teachings of Oishi in the Rowney system. Furthermore, Applicants submit that claim 1 is not obvious over the combination of these two references and in particular that Rowney is different from the description suggested by the Examiner. For these reasons, Applicants submit that claim 1 is allowable.

Concerning claim 2, the Examiner states that Rowney teaches that the validation is guaranteed by C and upon the guarantee invalidates unique transistory insignia. Applicants submit that Rowney does not teach that the validation is guaranteed by C but discloses that B verifies C's public key certificate to verify the legal identity of C. This has nothing to do with guaranteeing a payment transaction. Also, Rowney does not teach that C invalidates the insignia, but merely describes the SSL protocol.

Concerning claim 3, the Examiner states that Rowney suggests that a first time stamp is recorded by C. Applicants submit that Rowney does not suggest that the first time stamp is recorded by C, but discloses that A optionally transmits client certificate to B. This certificate described is a X.509 certificate and must be obtained from a certificate authority which requires the submission of certain personal information and takes a considerable amount of time.

Concerning claim 4, the Examiner suggests that a second time stamp is recorded by A. Applicants submit that Rowney does not suggest a second time stamp having the date and time when A, in order to verify the approval to B, associates the transaction with a verification insignia, but instead Rowney describes a complete normal and well-known capture exchange with a capture token which does not include a payment transaction.

Concerning claim 5, the Examiner states that Rowney suggests that the unique transistory insignia comprises the first time stamp. Applicant submit that Rowney does not suggest the unique transistory insignia comprising the first time stamp. As discussed in regard to claim 3, Rowney does not suggest a time stamp recorded by C.

Concerning claim 6, the Examiner states that Rowney suggests that the insignia is invalidated by C after a pre-specified time. Applicants submit that Rowney does not suggest that the insignia is invalidated by C after a pre-specified time. C is not mentioned at all in the reference and there is no invalidation of any insignia.

Concerning claim 7, the Examiner states that Rowney suggests that the time is between 10 milliseconds and 5 minutes. Applicants submit that Rowney does not suggest the pre-specified time in this range but merely makes a reference to programming languages like JAVA and C++ and to a user interface.

Concerning claim 8, the Examiner states that Rowney teaches verifying the correctness of the unique transistory insignia. Applicants submit that Rowney does not teach the verification of the correctness of the insignia, but rather describes that the merchant computer verifies the certificate of payment computer C. Rowney does not describe that A is verified or validated by

C. The communication described includes only the verification of the payment computer certificate by calling the certification authority.

Concerning claim 12, the Examiner states that Rowney teaches that the insignia has a unique identification number. Applicants submit that Rowney does not teach that the insignia has a unique identification number. The reference describes part of the SSL protocol where a certificate can be used an option.

Concerning claim 13, the Examiner states that Rowney suggests that the unique identification number is associated with a financial agreement. Applicants submit that Rowney does not suggest that the number is associated with a financial agreement but instead describes the SSL protocol and the optional certificate. A financial agreement is not mentioned at all.

Concerning claim 18, the Examiner states that Rowney teaches that C requests a payment by B, the request being associated with the insignia. Applicants submit that the Examiner has misunderstood the claim. The claim states that C is requested a payment by B, the request being associated with the insignia. In any case, Rowney does not teach that C is requested a payment by B with the request being associated with insignia, but rather merely describes the detailed steps of processing a payment capture request and generalizing and transmitting a payment capture request response. This is the normal exchange of information at the time when purchased items physically are being shipped to the customer. This exchange is a normal standard between financial institutions and is not part of the present invention.

Concerning claims 23, 26 and 27, Applicants submit that Rowney does not teach that the insignia is comprised in a digital code or that the pre-specified time is between 30 seconds and 4 minutes or suggests that the time is 2 minutes, but instead, Rowney only describes the SSL protocol and the certificate.

Claims 10, 24 and 25 stand rejected under 35 U.S.C. § 103 as being obvious over Rowney in view of Oishi and further in view of Puhl et al. (U.S. Patent 6,223,291). This rejection is respectfully traversed.

The Examiner relies on Puhl et al. to teach a network that uses a wireless application protocol such as WAP protocol. The Examiner feels that it would have been obvious to modify the teachings of Rowney and Oishi so that the network is implemented using a wireless application protocol.

Applicants submit that Puhl et al. teaches a network that is adapted to use a wireless application protocol. However, Puhl et al. describes a system for secure downloading of content items for wireless phones and maintaining content certificates for licenses for the content items. It does not describe the secure payment system but instead describes the use of license certificates which allows devices such as wireless phones to upload specified software products. Puhl et al. does not teach that the digital code is generated in a cellular phone by means of a digital device provided by C, but describes the use of different kind of digital certificates which are generated and loaded into the phone at the factory.

For these reasons, Applicants submit that the combination of these three references does not teach the features of claims 10, 24, and 25.

Claim 11 stands rejected under 35 U.S.C. § 103 as being obvious over Rowney in view of Oishi and further in view of Aziz (U.S. Patent 6,223,291). The rejection is respectfully traversed.

The Examiner cites Aziz to teach a secure communication channel on the Internet protected by a secret identification code. Applicants submit that Aziz does not teach that the insignia is transmitted over the Internet through a secure communication channel protected by a secret identification code, but instead describes the use of an anonymous file transfer protocol together with a user's electronic email name which is sent to a destination server. The use of a file transfer protocol does not secure the communication channel. Furthermore, using an email name as a password is not a very secure means of identifying a client computer as email names are not protected in any manner.

Claim 22 stands rejected under 35 U.S.C. § 103 as being obvious over Rowney in view of Oishi and further in view of Haber et al. (U.S. Patent 5,136,646). This rejection is respectfully traversed.

The Examiner cites Haber et al. to teach that a unique identification number is selected from numbers agreed between C and the trusted partners of C. Applicants submit that Haber et al. does not teach that the unique identification number is selected from a pool of numbers, but instead Haber et al. describes an identification process of digital documents from different authors performing certain calculations on the document including a transaction number and generating a time stamp receipt which is sent back to the author of the document. There is no mention of any pool of numbers agreed between C and the trusted partners of C. The transaction number is a sequential number per document received by the time stamping authority and assigned thereby. Consequently, Haber et al. does not teach that the number is released after the transistory insignia has been invalidated but rather describes the preparation steps for receipt of the document.

Claims 14, 20 and 21 stand rejected under 35 U.S.C. § 103 as being obvious over Rowney and Oishi in view of Franklin et al. (U.S. Patent 5,883,810). This rejection is respectfully traversed.

The Examiner states that Franklin et al. teaches that the financial agreement includes the trusted partner of C providing A with a payment card. The unique number is selected in accordance with a unique number of the payment card.

Applicants submit that Franklin et al. does not teach that the financial agreement includes the trusted partner of C providing A with a payment card, but rather teaches that the issuing bank issues an online commerce card to the customer in the form of a signed digital certificate and a software module that can be invoked when using the commerce card to conduct a transaction on the Internet. The consequence of this is that a customer waiting to conduct a purchase on the Internet must have a signed digital certificate from the financial institution and a software module loaded down in the customers computer. Then, the customer must invoke the software module to prepare a request for transaction number and digitally signs the request using the customer's private key and submits the signed request to the issuing banks computer. The request contains a certificate originally issued by the bank. Franklin et al. does not teach that the unique number is selected in accordance with the unique number of the credit card nor does Franklin et al. teach that the unique number is selected in accordance with the unique issuer identification number of C or in accordance with a unique identification number of a trusted partner of C.

The present invention is different from Franklin et al. in that it does not require any software module to be downloaded to the customer computer and does not require issuing a signed digital certificate stored on the customer computer. The fact that a specific software module from the issuing bank and original certificate must be stored on the customer computer makes the system described by Franklin et al. unsecure in the sense that it is vulnerable for misuse in that the customer computer can be stolen and in turn can use the customer computer to make false purchases or a thief can make a copy of the disk and distribute it to other people. Accordingly, Applicants submit that these claims are likewise allowable.

Claims 15-17 and 19 stand rejected under 35 U.S.C. § 103 as being obvious over Rowney in view of Oishi and further in view of Collin (U.S. Patent 6,223,291). This rejection is respectfully traversed.

The Examiner relies on Collin to teach a unique identification number which comprises at least a first and a second identification component. The Examiner states that Collin further teaches that the first identification component identifies a financial agreement and the second identifies C. Applicants submit that Collin does not teach that the unique identification number has two identification components. Collin does not teach that the first component identifies the financial agreement and the second identification component identifies C. Instead, Collin describes a coding zone in memory for coding a sequence of value units which are spaced apart at successive powers of two which correspond to the monetary amounts. Collin does not teach that the second identification component is assigned to C by a registration authority agreed upon, but instead Collin describes that the microchip card includes an internal microprocessor capable of performing all of the operations relating to transactions on its own and is also capable of loading and reloading the card with value units and giving change automatically. Further, Collin does not teach that there is an interdependency between the financial agreement and a disbursement account, but instead describes that during a transaction, the microprocessor card may send a transaction certificate to the trader's terminal in order to verify the validity of the card. There is no mentioning of a financial agreement or a disbursement account and there is no mention of a payment being withdrawn from a disbursement account.

Furthermore, Applicants note that the solution suggested by the present invention has not been produced by anyone. Credit card companies are still fighting against fraud due to stolen credit card numbers on the internet with the loss being counted in millions of dollars every year. Recently hackers have obtained close to 40 million credit card numbers and already thousands of cases of false purchases have been reported. The present invention is designed to eliminate these problems. No one has yet come up with such a solution to solve this important and growing problem.

CONCLUSION

In view of the above remarks, it is believed that the claims currently distinguish over the patents relied on by the Examiner either alone or in combination. In view of this amendment, reconsideration of the rejections and allowance of all the claims are respectfully requested.

If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone Robert F. Gnuse, Registration No. 27,295, at (703) 205-8000, in the Washington, D.C. area. Prompt and favorable consideration of this Amendment is respectfully requested.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Dated: June 29, 2005

Respectfully submitted,

By ROBERT F GNUSE
fr Joe McKinney Muncy 27295
Registration No.: 32,334
BIRCH, STEWART, KOLASCH & BIRCH, LLP
8110 Gatehouse Rd
Suite 100 East
P.O. Box 747
Falls Church, Virginia 22040-0747
(703) 205-8000
Attorney for Applicant